Functional Series 500 Management Services

Chapter 552 Classified Automated Information Systems Security

ADS 567

ADS 568

* **Standard Form 312, Classified Information Nondisclosure Agreement**

12 FAM 090

12 FAM 500

12 FAM 540

* **12 FAM 630**

* **12 FAM 640**

Functional Series 500 Management Services
Chapter 552 Classified Automated Information Systems Security

***552.1** Authority

1. The Omnibus Diplomatic Security and Anti-terrorism Act of 1986, as amended
2. The Computer Security Act of 1987, Public Law 100-235, as amended by Public Law 104-106, National Defense Authorization Act (Fiscal Year 1996) Division E, Information Technology Management Reform (Clinger-Cohen Act)
3. The Freedom of Information Act of 1966, Public Law 89-554, as amended.
4. Section 587 of the Fiscal Year 1999 Omnibus Appropriations Act, Public Law 105-277, as amended
5. The Privacy Act of 1974, Public Law 93-579, as amended
6. The Computer Fraud and Abuse Act of 1986, Public Law 99-474, as amended by the National Information Infrastructure Protection Act of 1996, Public Law 104-294

* 7. Executive Orders **10450, "Security requirements for Government employment," 12656, "Assignment of Emergency Preparedness Responsibilities,"** 12829, "National Industrial Security Program" (as amended), 12958, "Classified National Security Information" (as amended), 12968, "Access to Classified Information," 13011, "Federal Information Technology," and 13103, "Computer Software Piracy" as amended

* 8. 32 Code of Federal Regulations (CFR) **Part 154, "Department of Defense Personnel Security Program Regulation" and** Part 2004, "Safeguarding Classified National Security Information" and associated implementing guidance

9. Foreign Affairs Handbook, 12 FAH-6 (OSPB Security Standards and Policy Handbook)

* **10. DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)**

11. DOD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria"
12. 12 Foreign Affairs Manual 090, Definitions of Diplomatic Security Terms
13. 12 Foreign Affairs Manual 500, Information Security

* **14. 12 Foreign Affairs Manual 630, Classified Automated Information Systems**

* **15. 12 Foreign Affairs Manual 640, Domestic and Overseas Automated Information Systems Connectivity**

552.2 Objective

To outline the Agency's Classified Automated Information Systems (AIS) Security Program framework.

552.3 Responsibility

1. The Administrator is the Agency’s senior official. In this capacity the Administrator is responsible for developing and implementing a comprehensive, Agency-wide information systems security program that is technically current, cost-effective and in full compliance with established national security directives. This responsibility has been delegated to the Bureau for Management, Office of Information Resources Management (M/IRM).

2. The Assistant Administrator, Bureau for Management (AA/M) or the Chief Information Officer (CIO), by delegation of authority, is responsible for directing, managing and providing policy guidance and oversight with respect to all Agency information resource management activities. These responsibilities may be delegated to senior level office managers.

3. The Bureau for Management, Office of Information Resources Management (M/IRM) is responsible for providing "signatory approval to operate" for all automated information systems used to process, store or print sensitive but unclassified information. The Director of M/IRM has the authority to approve, subsequent to coordination with the Director of the Office of Security (D/SEC), the use of all automated information systems used to process, store or print classified national security information.

The Director of M/IRM has been assigned responsibility for management and oversight of Agency information system resource programs; and for compliance with federal regulations related to paperwork reduction, TEMPEST, Communications Security (COMSEC), and operational security for secure telephone units.

4. The Information Systems Security Officer (ISSO) for USAID is designated by the Administrator and is directly responsible for the following:

a. Reporting on all Agency information systems security issues to the Director of M/IRM;

b. Reviewing and coordinating all requests for exemptions to the Agency's information systems security policy as explained in this ADS chapter;

c. Directing inquiries into suspected security incidents involving automated system assets;

d. Coordinating investigations, with the Office of Security, of all suspected computer security violations, incidents, and compromises of classified national security information;

e. Coordinating and/or participating in actions taken as a result of suspected or proven security incidents involving automated information systems;

f. Serving as the primary point of contact for automated information systems security issues and inquiries for site information systems security officers throughout the Agency;

g. Providing the information technology security interface between M/IRM divisions and other Agency organizations; and

h. Representing the Agency in inter-governmental and inter-agency organizations and specialized groups at the working group level.

5. The Bureau for Management, Office of Information Resources Management, Telecommunications and Computer Operations Division (M/IRM/TCO) is directly responsible for ensuring each Agency facility is supported by telecommunication and computer resources capable of operating in compliance with the Agency's information systems security program and policy.

6. The Bureau for Management, Office of Information Resources Management, Systems Development and Maintenance Division (M/IRM/SDM) is directly responsible for the following:

a. Ensuring corporate application software and system maintenance resources are capable of operating in compliance with the Agency's information systems security program policy and;

b. Ensuring operational and functional software security controls are provided for the technical enforcement of need-to-know restrictions on all automated information system equipment operating in a distributed or network mode.

7. The Bureau for Management, Office of Information Resources Management, and the ISSO for USAID are directly responsible for the following:

   a. Addressing computer and communications security issues during system migration planning, system architecture planning, information engineering, and new system technology research and development;

   b. Incorporating computer and communications security as an evaluation element in the overall Agency information management (IM) quality assurance program;

   c. Coordinating the development of contract security classification specifications (DD Form 254 or equivalent) for maintenance and service contracts supporting classified automated information systems with the Office of Security (SEC) and the Office of Procurement (M/OP);

   d. Developing and implementing the Agency's information systems security program;

   e. Assisting in the accomplishment of risk, sensitivity or vulnerability assessments in support of systems life-cycle activities or continuing Agency risk management, and coordinating, when appropriate, the resulting reports at or above the division chief level;

   f. Developing, implementing and supporting an Agency-wide automated information systems security awareness and education program;

   g. Ordering and coordinating the installation of secure telephone unit (STU)-III units in Agency facilities with the Department of State COMSEC Accountant; and

   h. Maintaining COMSEC accountability, keeping an up-to-date inventory of STU-III systems and other controlled cryptographic items, as well as instituting a cryptographic key management procedure.

8. Information Technology (IT) Specialists (USAID/W), System Managers (USAID Missions) and system staff are directly

responsible for the following:

a. Ensuring all automated information systems under their cognizance are operated, on a day-to-day basis, in compliance with the Agency's information systems security policy and guidelines as promulgated in this chapter;

b. Coordinating with the system staff implementation of information systems security standards for automated information systems;

c. Providing the site ISSO with technical support and expertise in the implementation of Agency information systems security policies;

d. Maintaining an inventory of all hardware, operating system software, application software, peripheral devices, and communication links that are part of the system(s) within their purview, and reporting all incidents of lost or stolen equipment to the appropriate security office; and

e. Disseminating the Agency's system security policies, procedures and guidelines to all users of the system under their purview.

9. The COMSEC Custodian and Alternate are cleared, U.S. citizen, direct-hire employees of the Agency who are designated by either M/IRM (USAID/W) or Mission Directors/Representatives and are directly responsible for the following:

a. Ordering cryptographic keys;

b. Managing keying material and STU-III equipment accounting services in accordance with mandatory procedures delineated in NTISSI No. 4001/CSISM/CCI;

c. Ensuring facility/mission compliance with national and Agency communication policy (**See 545.5.4**); and

d. Assisting the ISSO for USAID in maintaining COMSEC accountability, keeping an up-to-date inventory of STU-III systems and instituting a cryptographic key management procedure.

e. Coordinating investigations of lost or suspected loss of

COMSEC or cryptographic equipment and materials with the Office of Security (SEC.)

10. The Bureau for Management, Office of Human Resources (M/HR) is directly responsible for ensuring that position descriptions reflect information systems security responsibilities.

11. Program Managers are directly responsible for the following:

a. Determining which system users have a verifiable need to access applications, programs, and sub-programs used to support their job tasks and responsibilities, and informing the IT Specialist/ System Manager, in writing, of all system access requirements;

b. Informing the designated ISSO of any security incidents related to software applications supporting their program or system users;

c. Appointing, in writing, a U.S. citizen who is a direct-hire Agency employee to serve as designated ISSO for each automated information system supporting their program tasks and responsibilities, or within their purview; and

d. Managing the overall automated information systems security program for their functional areas, including the implementation of all applicable information systems security policies and guidelines as described in this chapter.

12. The designated ISSO and alternate are appointed by the Program Manager or the IT Specialist's first-line supervisor at USAID/W. The Mission Executive Officer (EXO) acts as the designated ISSO at the missions. The designated ISSO is responsible for the following:

a. Implementing Agency information systems security policy and guidelines as directed in this chapter and as it applies to automated information systems under the designated ISSO's cognizance;

b. Keeping the Mission Director/Representative, System Manager, ISSO for USAID, and other facility security personnel apprised of all suspected or known security incidents, violations, and/or compromises associated with the automated information system under the ISSO's cognizance;

c. Providing technical assistance during system security investigations conducted by authorized Agency personnel or bona fide representatives;

d. Conducting basic security awareness training for end-user personnel authorized to access the automated information system under their purview;

e. Conducting annual self-evaluation reviews of the automated information systems security program under their purview; and

f. Coordinating with the Department of State's embassy or consulate ISSO, Regional Security Officer **(RSO)**, and/or Security Engineering Officer on all issues associated with automation security.

13. Users of USAID information systems are directly responsible for the following:

a. Abiding by Agency information systems security polices and guidelines as directed in this chapter; and

b. Reporting system or application irregularities or suspected security violations to the Program Manager, Mission Director/ Representative, designated ISSO, or System Manager/ Administrator.

14. The Director, Office of Security is responsible for the following:

a. Coordinating with the ISSO for USAID the reporting and investigation of suspected or known automated information systems (AIS) security incidents, violations, and compromises, including those involving COMSEC and cryptographic equipment and materials;

b. Performing inspections of USAID information systems to ensure classified national security information is properly protected;

c. Conducting background checks on all U.S. citizens requesting access to USAID systems that process, store, or control sensitive information (**See ADS 567**);

d. Approving, in coordination with the Director, M/IRM, the authority of an overseas mission and USAID/Washington Bureau/

Independent Office to process classified national security information on an information technology system.

552.4 Definitions **(See Glossary)**

Classified National Security Information (Classified Information):
Compartmented
CONFIDENTIAL
dedicated mode
encryption
SECRET
STU III
TEMPEST
TOP SECRET

552.5 POLICY

The statements contained in the .5 section of this ADS chapter are the official Agency policies and corresponding essential procedures.

*552.5.1 CLASSIFIED AUTOMATED INFORMATION SYSTEMS (AIS) PROTECTION

It is the policy of the United States Agency for International Development (USAID) to protect the Agency's electronic information commensurate with the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of such information. All data of value to the Agency requires some minimum level of protection. Certain data, because of the sensitivity or criticality of the information to the mission of USAID, require additional safeguards. **Failure to protect Classified National Security Information (Classified Information) can lead to adverse administrative actions, and both civil and criminal penalties.**

E552.5.1 Classified Automated Information Systems (AIS) Protection - N/A

*552.5.1.a INFORMATION SYSTEMS SECURITY PROGRAM

The Agency's policy is to implement and maintain an information systems security (ISS) program to ensure that adequate computer security is provided to all Agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. All USAID networked computer systems **and stand-alone terminals used to process classified data** shall provide controlled access protection safeguards to protect the integrity, availability, and where required, the confidentiality of Agency information.

***E552.5.1a** Information Systems Security Program

USAID's ISS Program implements policies, standards and procedures that are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration, **the Department of Defense, the Department of State, the Information Security Oversight Office (ISOO)** and the Office of Personnel Management (OPM). Different, more stringent requirements for securing national security information will be incorporated into USAID classified programs as required by appropriate national security directives. Classified processing requirements do not apply to unclassified systems. However, at a minimum, USAID's ISS program requires that the controls outlined in OMB A-130, Appendix III must be implemented in all Agency general support and major applications systems.

552.5.1b ACCESS TO CLASSIFIED AIS NETWORKS

USAID's security policy, for access to classified USAID computer networks, is designed to protect sensitive Agency information against unauthorized access or disclosure using formal authorized access permission procedures. These procedures are based on a clearly demonstrated need to know or need to use policy supported by an approved personnel screening process and formal authorization approval which, when used together, implement the USAID security policy for USAID System access.

E552.5.1b Access to Classified AIS Networks - N/A

552.5.2 CLASSIFIED INFORMATION PROCESSING

E552.5.2 Classified Information Processing - N/A

***552.5.2a** CLASSIFIED INFORMATION PROCESSING - OVERSEAS

The requirements for processing of classified national security information overseas are contained in 12 FAH-6 (12 Foreign Affairs Handbook-6, OSPB Security Standards and Policy Handbook). No classified information processing will be authorized at an overseas mission without the approval of the Office of Security (SEC) and M/IRM. **(See also ADS 562, Physical Security Programs and mandatory**

references 12 FAM 630, Classified Automated Information Systems and 12 FAM 640, Domestic and Overseas Automated Information Systems Connectivity.)

E552.5.2a Classified Information Processing – Overseas - N/A

***552.5.2b** CLASSIFIED INFORMATION PROCESSING – USAID/WASHINGTON

Processing classified national security information will only be accomplished within Restricted Areas. Equipment used for such processing will not be removed from the Restricted Area without coordination with M/IRM, SEC and the ISSO. **(See also ADS 562, Physical Security Programs and ADS 565 Physical Security Programs (Domestic)) (See ADS 562 and ADS 565)**

Program Managers, IT Specialists, supervisory personnel and end-users having responsibilities, duties, or tasks in support of USAID must adhere to the following personnel, technical, administrative, and physical security policies when equipment, approved to process classified information, is used to support program activities and mission objectives. **(See also ADS 561 Security Responsibilities, ADS 566 U.S. Direct-Hire and PASA/RSSA Personnel Security Program, ADS 567 Classified Contract Security and Contractor Personnel Security Program and ADS 568 National Security Information and Counterintelligence Security Program.) (See ADS 561, ADS 566, ADS 567 and ADS 568)**

***** **The Office of Security (SEC) conducts background investigations for USAID direct-hires. Because the Defense Security Service (DSS) conducts background investigations on USAID institutional contractors, and is also responsible for oversight of contractor facilities where classified data is stored and/or processed, some applicable security policies and procedures can be found in 32 CFR Part 154, Department of Defense Personnel Security Program Regulation, and Department of Defense Manual DoD 522.22-M, National Security Program Operating Manual. Additional specifics on Defense-related security requirements can be found in the Supplemental Reference "Selected Security Guidance."**

E552.5.2b Classified Information Processing – USAID/Washington - N/A

***552.5.2c** PERSONNEL REQUIREMENTS

1) Security Clearances

* All personnel accessing USAID classified automated information systems must have **the following:**

- **A** security clearance commensurate with the highest classification of information ever processed or stored on the system**;**
- **T**he appropriate access levels**;**
- **A** need-to-know in connection with the performance of official duties**;**
- **A completed Standard Form 312, Classified Information Nondisclosure Agreement,** and
- **K**nowledge of their computer responsibilities.

(See E552.5.1a. See also ADS 561 Security Responsibilities, ADS 566 U.S. Direct-Hire and PASA/RSSA Personnel Security Program, ADS 567 Classified Contract Security and Contractor Personnel Security Program and SF -312)

2) Personnel Management

* a. **R**esponsible supervisors shall ensure that a statement establishing responsibilities for **classified** information systems security is included in position descriptions for the ISSO for USAID, designated ISSOs, IT Specialists, members of system staffs, Program Managers, System Managers, and any other personnel having a direct responsibility for safeguarding Agency computer systems. **M/HR/POD staff are available to assist supervisors in the development of position descriptions.**

b. Visitors, custodial, and facility maintenance personnel who are inside restricted areas, without security clearances, must be escorted and kept under continuous observation by personnel authorized unescorted access to those areas.

***E552.5.2c** Personnel Requirements

1) The procedures for requesting security clearances are contained in ADS 566 U.S. Direct-Hire and PASA/RSSA Personnel Security Program and 567 Classified Contract Security and Contractor Personnel Security Program. **(See ADS 566 and ADS 567)**

* 2) The IT Specialist must ensure all vendor maintenance and customer support personnel are cleared at a level commensurate with the highest classification of information authorized to be processed on the equipment. **All requirements specified in paragraph 552.5.2c paragraph 1) apply to vendor maintenance and customer support personnel who may access classified data in the course of their activities.**

***552.5.2d** TECHNICAL SECURITY

USAID offices and bureaus must control access to specialized system software, utilities, and functionality that could be used to gain unauthorized access to application data and program code. Classified information systems must be operated in accordance with the following policies:

1) Classified information must be processed on dedicated, stand-alone computer systems approved by M/IRM Security to process such information. The processing, storing, printing, or transmitting of classified information on any network, distributed system, or mainframe computer system is strictly prohibited. Exemptions to this policy must be approved by M/IRM. **(See E545.5.2d and ADS 568 National Security Information and Counterintelligence Security Program.)**

2) Users must not install personally owned software, shareware, or freeware on classified systems owned or operated by the Agency**.**

3) Users must not install or use personally owned computers, communication devices, printers, or other peripheral computing devices in facilities housing computer systems approved to process classified information. (**See ADS 550 End-user Applications)**

4) All operating system and application software must reside on removable drives.

E552.5.2d Technical Security

1) Computer systems approved to process classified information must not be connected to any other information system.

2) There are no requirements for TEMPEST protection within USAID/W facilities. However, a one-meter (39.37 inches) separation must be maintained between computer systems and printers approved to process classified information and other electronic and telephonic equipment.

M/IRM will provide requestors with acceptable TEMPEST protected automated information system equipment.

***552.5.2e** ADMINISTRATIVE SECURITY

Access to automated information systems approved to process classified information must be restricted to individuals requiring such access to perform official duties. The level of access granted must limit users to only the information needed to complete assigned responsibilities. **Prior to permitting access to classified data, supervisors must ensure the individual has executed a Standard Form 312, Classified Information Nondisclosure Agreement.** The following policies must be followed to facilitate access controls. **(See ADS 568 National Security Information and Counterintelligence Security Program and SF 312)**

1) Appointment of ISSOs and Alternates - **User Approval**

a. The Administrator or the CIO shall designate, in writing, an Agency employee to serve as the ISSO for USAID. The designee must have at least a TOP SECRET security clearance and be a U.S. citizen direct-hire employee.

b. Program Managers shall appoint, in writing, a designated ISSO and alternate to manage the automated information systems security program for their organizational entity. An appointment letter shall be sent to the ISSO for USAID. Both designees must be U.S. citizen direct-hire employees of the Agency and have at least a SECRET security clearance.

c. Users approved by the ISSO to process classified information must sign and complete a USAID Classified Automated Information System Users Agreement **(See Supplementary Reference, USAID Classified Automated Information System User Agreement)** This form shall be retained in a central file for up to six months. In no case shall foreign nationals be given authorization to process or access classified information.

2) Access to Computer Systems Approved to Process Classified Information

a. Program Managers shall determine who within their organizational entity requires access to computers approved to process classified information. This determination shall be in writing and based on a valid need-to-know **(See Supplementary Reference, Approval to Access and Process Classified National Security Information via Automated Information Systems Equipment)**

b. Prior to receiving authorization to process classified information, the user must receive classified information processing and handling instructions from either the ISSO for USAID or the designated ISSO.

c. In no case shall foreign nationals be given authorization to process or access classified information.

* **d. The element IT Specialist/System Manager must maintain a visitors log for all properly cleared persons not normally assigned to the area where classified data processing is taking place. Individuals not on the "Authorized Access List" must sign the visitors log prior to being allowed access to any system which is approved for processing classified data. Visitors must be under continuous visual observation by a person with authorized unescorted access (See Supplementary References, Authorized Access List, and Visitors Log)**

* 3) Use of Systems Approved to Process Classified

Information

a. **The guidance in this chapter only applies to USAID computer systems and networks approved to process information classified at the SECRET or CONFIDENTIAL level. Additional guidance on processing data which is classified TOP SECRET or which requires special handling (e.g., compartmented data or special access program data) is available from the Office of Security.**

b. Personal use of Agency automated information systems approved to process classified information is prohibited.

4) Protecting Information Displayed and Processed on Classified Systems

a. Video screens displaying classified information must be protected in the same manner as other classified material, or other equipment. **(See E545.5.2e paragraph 4)a) and ADS 568)**

b. Removable data storage media (e.g., floppy disks, removable hard disks, tape drives, etc.) containing classified information must not be left unsecured or resident in a computer system when the computer system is unattended by personnel authorized to process classified information. **All media containing classified material must be properly marked.**

c. Users must ensure classified files are not stored in a printer's queue or spool file, and classified information is not left unattended in a printer.

5) Labeling

a. Labels indicating the highest classification level of information approved for processing on the system must be affixed to computer devices and removable media. **(See ADS 568 and 12 FAM 500)**

b. Documents, files or records containing classified information must not be initially processed on unclassified systems then subsequently labeled or marked as classified data.

6) Protection of Media and Output

a. The Program Manager, designated ISSO and users must ensure all media used to produce classified hard copy material are protected in accordance with ADS 562, Physical Security Programs, ADS 568 National Security Information and Counterintelligence Security Program, and the policies provided in this chapter. **(See ADS 562 and ADS 568)**

b. The designated ISSO or the ISSO for USAID must inform users of their duties in protecting classified media and hard-copy output. **(See ADS 561 Security Responsibilities)**

7) Disposal of Classified Media and Output

Destruction of removable media and classified output shall be carried out by cleared U.S. personnel and accomplished by shredding or placing the material in a separate burn bag marked "Electronic Media."

8) Violations

a. The **Office of Security (SEC)** must investigate all suspected or known security incidents and violations involving information systems. **(See ADS 568 National Security Information and Counterintelligence Security Program)**

b. The designated ISSO shall randomly review selected storage media and system hardware associated with automated information systems under their purview to ensure users are not processing information classified above the level authorized for the system, and that classified information is not being processed on unauthorized system equipment.

9) System Maintenance

a. Personnel who perform system maintenance must have a security clearance commensurate with the highest level of information approved for processing on the computer system**. (See ADS 566 U.S. Direct-Hire and PASA/RSSA Personnel Security Program and 567 Classified Contract Security and Contractor Personnel Security Program)**

b. The designated ISSO shall maintain a log of all maintenance service performed on automated information system equipment approved to process classified information.

c. A suitably cleared and knowledgeable person must supervise vendor maintenance personnel accessing computer systems approved to process classified information and ensure that maintenance personnel do not remove any storage media that have ever been used in conjunction with system equipment approved to process classified information.

d. Only U.S. citizen personnel who have TOP SECRET clearance and M/IRM authorization are allowed to maintain TEMPEST equipment.

10) Record Keeping

The designated ISSO must ensure the original automated information system (AIS) security documents, logs and records listed below are maintained, after processing, in a central file for each system authorized to process classified information:

- Classified System User Agreements and Termination Notices;
- Contingency Operation, Disaster Recovery, and Emergency Action Plans;
- Copies of Waivers or Exceptions;
- System Certification;
- System Maintenance Log;
- Security Reviews;
- Designated ISSO and Alternate Appointment;
- Annual Security Compliance Review; and

- o System Inventory.

11) Security Reviews

a. The designated ISSO must ensure computer systems approved to process classified information are installed in accordance with the National COMSEC Information Memorandum (NACSIM 5203), "Guidelines for Facility Design and RED/BLACK Installation," available from the ISSO for USAID.

b. The designated ISSO, in conjunction with the Program Manager and other appropriate Agency personnel shall conduct an annual review of user and automated information systems operating practices to evaluate compliance with Agency security policies.

c. The ISSO for USAID shall conduct or direct the conduct of security evaluations of computer systems authorized to process classified information not less than every three years. These evaluations shall address compliance with applicable Federal and Agency information systems security policies, standards, and requirements.

12) Training

a. The ISSO for USAID must provide security training to designated ISSOs, Program Managers, and users authorized to process classified information. Upon request, the ISSO for USAID shall provide special training for other Agency personnel having security responsibilities for Agency classified systems.

b. The designated ISSO must ensure annual computer security awareness training is provided to all USAID classified system users.

c. The designated ISSO will provide annual training in Washington or at the missions and must address application-specific security measures.

13) Backup, Emergency Action, and Contingency Operation Planning

a. Users shall backup all files retained on removable media, and ensure such media are secured in approved security containers when not in use.

b. Program Managers and the designated ISSO must develop, test, and implement emergency action plans for each facility accommodating an automated information system approved to process classified information.

c. The designated ISSO shall develop site-specific Disaster Recovery Plans based on threat identification information, system resource accounting, and criticality assessment data.

14) System Certification

No classified data or information shall be processed using system equipment unless the system has been accredited by the appropriate approving authority. **(See Supplementary Reference, Automated Information System Certification and Approval to Operate)**

***E552.5.2e** Administrative Security

1) Appointment of ISSOs and Alternates

* Section currently under development. ***(Projected topic deals with documentation of appointees.)***

2) Access to Computer Systems Approved to Process Classified Information

* Section currently under development. ***(Projected topics deal with annual review by Program Managers for personnel under their supervision and user documentation procedures.)***

3) Use of Systems Approved to Process Classified Information

* Section currently under development. ***(Projected topics deal with appropriate points of contact for guidance on systems use, and personnel authorized to conduct spot check of classified AIS systems to ensure appropriate standards are followed by users.)***

4) Protecting Information Displayed and Processed on Classified Systems

a. Users must ensure that no classified information is displayed on a screen when unauthorized or uncleared individuals are physically positioned to view the screen. The designated ISSO must ensure workstations located in high access areas or those exposed to potential public viewing are equipped with screens that restrict the angle of viewing. Workstation screens must face away from windows and open access areas to prevent casual viewing of screens by unauthorized or uncleared individuals.

* b. Section currently under development. ***(Projected topic deals with users' protection of information processed on classified systems.)***

5) Labeling

a. The designated ISSO must ensure each device associated with a computer system approved to process, store, or print classified information is prominently labeled to indicate the highest classification level of information approved for the system.

In addition to displaying the highest classification level of information approved for the system, classified system device labels must also indicate the name and phone number of the designated ISSO responsible for the security of that unit of equipment.

b. Users shall affix labels to all removable media (i.e., floppy disks, removable hard disks, etc.) indicating the highest level of information approved for processing on the system.

Labels for removable media indicating the highest level of information approved for processing on the system are ordered from GSA (FEDSTRIP) using the following National Stock Numbers:

o SECRET	Label (SF) 707	7540-01-207-5537
o CONFIDENTIAL	Label (SF) 708	7540-01-207-5538

o UNCLASSIFIED Label (SF) 710 7540-01-207-5539.

6) Protection of Media and Output

Documentation and removable media (e.g., floppy disks, removable hard disks, etc.) shall be stored in an approved security container.

7) System Maintenance

a. At the missions, the EXO shall maintain a log of all maintenance services performed on system equipment approved to process classified information.

b. Classified, automated information systems maintenance logs must include the date of service, service performed, hardware or software involved, names of individual(s) performing service, equipment removed or replaced, and system condition or status following the service. All maintenance log records must be retained in the central system file for a period of six months after the date of entry.

c. Maintenance personnel are prohibited from running remote diagnostics on any Agency computer system approved to process classified information.

d. Maintenance personnel must not remove from Agency premises any hardware, software, or magnetic media that has been used in association with computer systems approved to process classified information without the expressed written permission of the designated ISSO.

8) Record Keeping

Sample copies and instructions for the development and completion of many of the AIS security documents, logs and records are provided in the Supplementary References section of this chapter. **(See 552.6)**

9) Security Reviews

a. The classified automated information systems compliance review shall address personnel, administrative, technical, and physical security practices. **(See Supplementary Reference, Classified Processing Compliance Review)** The results of the review shall be retained in the central system file with a copy forwarded to the ISSO for USAID annually.

b. Each classified AIS security evaluation shall result in a draft report delineating findings and recommendations of the ISSO for USAID. The final report shall be distributed to the Program Manager, the appropriate office director, M/IRM and the Office of Security. **The results of a classified automated information systems compliance review, which may identify USAID vulnerabilities, should be appropriately marked for those with a need to know (e.g., banner the top of each page "Release Restricted-Verify Need to Know Before Permitting Access") in addition to other administrative markings (such as Sensitive Unclassified Information, CONFIDENTIAL, SECRET, TOP SECRET, NOFORN, NOCONTRACT, etc.)appropriate to the content of the document.) Additional information on Sensitive But Unclassified (SBU) Information can be found in 12 FAM 540 (See 12 FAM 540)**

10) Training

a. The ISSO for USAID shall make available specialized automated information systems security training for the designated ISSOs.

b. The designated ISSO must ensure personnel without security awareness training are not permitted access to systems authorized to process classified information. Furthermore, the designated ISSO is responsible for assuring that annual security awareness training is provided to all classified system users.

11) Backup, Emergency Action, and Contingency Operation Planning

a. Emergency action plans must be coordinated with the ISSO for USAID and be consistent with applicable Agency and local government emergency action plans. These plans must be developed in coordination with the designated ISSO. **(See also ADS 545, ADS 530 Emergency Planning Overseas and ADS 531 Continuity of Operations Program)**

b. Program Managers and designated ISSOs must review, update (if necessary), and test all emergency action plans annually, or when significant modifications are made to system hardware, software, or system personnel.

c. The designated ISSO shall retain copies of the most recent emergency action and contingency operation plans in the system's central file and at a backup site.

552.5.2f PHYSICAL SECURITY

Users must adhere to the following policies to ensure classified automated information systems are afforded the physical protection required for the highest classification level and most restrictive category of data or information stored or processed on the system. **(See ADS 562 Physical Security Programs and ADS 565 Physical Security Programs (Domestic))**

1) A computer system approved to process classified information shall only be located within a Restricted Area. **(See ADS 565)**

2) The IT Specialist and designated ISSO shall maintain a complete and up-to-date inventory of all system components and peripheral system devices within their location.

3) At the conclusion of each business day, the designated ISSO shall conduct or direct the accomplishment of an end-of-day security check of all work areas housing computer systems approved to process, store, or print classified information.

4) A laptop computer, without a removable hard drive, authorized to process classified information must be transported and stored in the same manner as classified information. For those laptops with removable hard drives, the drives must be stored in accordance with established procedures.

5) The Office of Security shall assist the requesting Bureau or Office by providing requirements for security measures. **(See ADS 568)**

*E552.5.2f Physical Security

1) Use of Computers for Processing Classified Data

a. Personnel with access to computer systems owned or operated by USAID must ensure the protection of information, equipment, and facilities. Violations of this section shall be enforced in accordance with ADS 568, National Security Information and Counterintelligence Security Program. (See ADS 568)

b. Classified information shall only be entered onto a system approved for processing such information. The creation, processing or storage of classified information on systems not approved for such purposes, is a security violation as defined in ADS 568, National Security Information and Counterintelligence Security Program. The limitations against retroactively classifying data also applies to documents prepared on automated information system equipment. (See ADS 568)

*** c. The designated ISSO must advise all system users to employ the most stringent access controls available (e.g., password protect, or process on a floppy disk using a stand-alone microcomputer) when processing classified information. Storage of such information on distributed or networked systems is prohibited. More details on classified information can be found in 12 FAM 090 Definitions of Diplomatic Security Terms. In addition, information systems security practices included in ADS 545 must be applied to classified automated information systems to the extent they are practicable. (See Mandatory Reference 12 FAM 090)**

2) Monitoring System Users

The designated ISSO shall conduct reviews of randomly selected user word processing documents, files, and floppy disks on a monthly basis to ensure users are adequately protecting classified information.

3) Security Incident Reporting

a. The IT Specialist/System Manager must document, in a system operation log, all security-related abnormal system operations such as unexplained changes in user or program access privileges, improper system responses to access control processes, or other hardware or software failures that result in unauthorized disclosure, data loss, or modification of system programs or data.

b. System users discovering or suspecting incidents of fraud, misuse, disclosure of information, destruction or modification of data, or unauthorized access attempts must immediately report such incidents to the designated ISSO and Program Manager (USAID/W) or the EXO (USAID Missions).

4) Violations

a. System users must not originate, process, print, or store classified information on any computer system not approved for that purpose. Individuals violating this provision shall be subject to the security violation procedures set forth in ADS 568, National Security Information and Counterintelligence Security Program. (See ADS 568)

b. Passwords to classified systems and sensitive data must be afforded a degree of protection commensurate with the magnitude of harm or loss that could result from inadvertent or deliberate disclosure. Employees disclosing passwords to classified systems are subject to administrative sanctions or disciplinary actions.

c. Program Managers, designated ISSOs and EXOs must take appropriate action to ensure security requirements for classified computer systems are met by all USAID personnel, contractors and vendors.

5) Emergency Action, and Contingency Operation Planning

a. M/IRM/TCO, in consultation with the Office of Security and the appropriate Program Managers, shall identify and secure, through a contractual agreement, facilities to store backup classified data and/or media to ensure continuity of operations for systems operating in USAID/W. Such facilities shall be off-site and employ appropriate environmental controls and alarm systems.

b. At mission locations, the System Manager, in consultation with the EXO, must identify a secure location to store backup classified data and media to ensure continuity of operations for all computers and computer peripherals used to process classified data which fall under the System Manager's purview.

c. The IT Specialist/System Manager and designated ISSO must develop emergency action plans for each facility accommodating a computer system operating under their purview in USAID/W. Such plans must be coordinated with the ISSO for USAID and be consistent with applicable Agency and local government emergency action plans (See Supplementary Reference, Contingency Planning for Information Resources)

d. The IT Specialist/System Manager and designated ISSO at a mission shall develop site-specific emergency action plans. (See Supplementary Reference, Contingency Planning for Information Resources)

e. The IT Specialist/System Manager and designated ISSO must review, update (if necessary), and test all emergency action plans annually, or when significant modifications are made to system hardware, software, or system personnel.

f. The ISSO for USAID shall develop site-specific contingency operation and disaster recovery plans based on threat identification information and system asset accounting and valuation data provided to the ISSO for USAID by the IT Specialist/System Manager and designated ISSO (See Supplementary Reference,

Contingency Planning for Information Resources)

g. Users must protect classified data processed in the stand-alone mode.

* **h. The Office of Security, in coordination with the RSO where appropriate, shall assist the requesting Bureau, Office, or mission in determining and installing appropriate physical security controls. (See ADS 562, Physical Security Programs, and ADS 565, Physical Security Programs (Domestic))**

552.5.3 HOST FACILITY SYSTEM SECURITY STANDARDS

The following policies apply when classified processing is performed at Agency facilities by non-Agency personnel or when Agency personnel must process classified information at other U.S. Government facilities.

1) When Agency facilities, organizations, personnel, or contractors are hosting U.S. cleared personnel not associated with USAID and classified processing is required, the computer security policies and procedures of USAID shall prevail.

2) When cleared U.S. personnel representing the Agency are processing classified information in U.S. Government facilities not operating under the auspices of USAID, the computer security policies and procedures of the host department or agency shall prevail.

3) If there is a conflict as to which computer security policies and procedures apply, the computer security policies and procedures of USAID shall prevail.

E552.5.3 Host Facility System Security Standards - N/A

552.5.3a SPECIAL CONSIDERATIONS FOR MISSIONS OPERATING IN CRITICAL TECHNICAL AND CRITICAL HUMAN INTELLIGENCE THREAT ENVIRONMENTS

Missions located in geographic areas bearing a critical technical and critical human intelligence threat designation (available from the Office of Security and ISSO for USAID on a need-to-know basis) must operate automated information systems approved to process classified information according to the following guidance:

1) System Access

Agency personnel requiring access to system supervisory functions must be at least SECRET cleared U.S. citizens.

2) Technical Security

Certain policies and procedures for system connectivity are designated as SBU and CONFIDENTIAL information. Therefore, they are not provided in this chapter. Location-specific policies and procedures for system connectivity are available from the EXO, RSO or ISSO for USAID.

3) System Software

a. System and application software shall not be locally procured.

b. Maintenance contractors and vendors must not use software that has been out of U.S. Government control unless it has been reviewed and approved by the ISSO for USAID.

c. Foreign nationals are not permitted to program or modify system or application software used in conjunction with distributed or networked systems.

d. The EXO must destroy all damaged or otherwise unusable floppy disks and tapes in accordance with approved local media destruction procedures determined by the RSO.

E552.5.3a Special Considerations for Missions Operating in Critical Technical and Critical Human Intelligence Threat Environments - N/A

552.5.4 CONNECTION OF SECURE TELEPHONE UNITS (STU-III) TO FAX EQUIPMENT

FAX communications involving classified information must be executed in conformance with the following security policies.

E552.5.4 Connection of Secure Telephone Units (STU-III) to FAX Equipment - N/A

552.5.4a PROCUREMENT OF STU-III

The following guidance must be adhered to when purchasing Secure Telephone Units (STU-III) and FAX Equipment in USAID/W and at missions:

1) FAX equipment to be connected to a secure telephone unit (STU-III) must be TEMPEST-approved and listed on the National Security Agency's Preferred Products List of the Endorsed TEMPEST Products List. Such products are procured through the ISSO for USAID.

2) FAX equipment that shall be connected to STU-III devices must not have data storage capability.

3) Only Type 1 STU-III devices listed on the National Security Agency's Preferred Products list shall be procured for classified data transmissions.

4) All STU-III and secure FAX devices are to be transported overseas by secure diplomatic pouch. Within the United States, such equipment must be transported by either registered U.S. mail or by U.S. citizens having at least a SECRET clearance.

E552.5.4a Procurement of STU-III - N/A

552.5.4b INSTALLATION AND REPAIR OF STU-III

The following requirements must be met when installing or repairing secure STU-III and FAX Equipment at USAID facilities:

1) The ISSO for USAID, in coordination with Office of Security, must approve the installation of all classified FAX devices within USAID/W facilities.

2) The communications security (COMSEC) custodian, in coordination with the RSO, must approve the installation of all classified FAX devices within USAID mission facilities.

3) The COMSEC custodian must ensure that the STU-III and

attached FAX equipment are located in an area approved to accommodate classified information and is configured correctly. **(See E545.5.4 paragraph 3))**

4) Maintenance on classified FAX and STU-III dataport connections must be performed by TOP SECRET-cleared U.S. citizen technicians.

E552.5.4b Installation and Repair of STU-III

STU-III devices must be connected to classified FAX devices by a data port. STU-III devices must not be configured to allow auto answer or auto secure.

For STU-III machines that allow data transmissions in the clear mode, the COMSEC custodian shall use the master crypto-ignition key (CIK) to configure the STU-III for encrypted mode processing only.

552.5.4c TRANSMISSIONS ON STU-III

The following requirements must be met when transmitting information using secure STU-III equipment connected to FAX Equipment in USAID/W and at missions:

1) Users must not allow data transmission in an unencrypted mode at any time during a STU-III and classified FAX connection.

2) Transmissions must be continuously observed during both the transmission and reception.

3) Users sending and receiving classified FAX transmissions must ensure terminal display information is correct and that transmissions do not exceed the classification level indicated on the terminal display.

E552.5.4c Transmissions on STU-III - N/A

552.5.4d ADMINISTRATIVE MANAGEMENT OF STU-III

The following administrative requirements must be implemented whenever secure STU-III equipment is connected to FAX equipment in USAID/W and at missions.

1) Labeling

a. The COMSEC custodian must ensure that FAX equipment authority to transmit classified information is clearly labeled, "EQUIPMENT IS AUTHORIZED FOR TRANSMISSION OF CLASSIFIED INFORMATION UP TO THE CONFIDENTIAL LEVEL," or "EQUIPMENT IS AUTHORIZED FOR TRANSMISSION OF CLASSIFIED INFORMATION UP TO THE SECRET LEVEL." **(See E552.5.4d paragraph 1)**

b. The COMSEC custodian must ensure the security requirements associated with operating classified FAX equipment are prominently posted near all functioning classified FAX equipment. **(See E552.5.4d paragraph 1))**

2) Personnel Responsibility

a. The COMSEC Custodian shall ensure that all personnel accessing communication devices authorized to transmit classified information have the required clearance levels and need-to-know in performance of their official duties, appropriate supervision, and knowledge of their communications security responsibilities.

b. The COMSEC Custodian is responsible for implementing applicable security policies for the protection of classified FAX equipment and transmissions.

c. Only the COMSEC custodian shall access the master crypto-ignition key (CIK).

d. The COMSEC custodian must ensure the STU-III terminals are keyed for the appropriate level prior to transmitting classified information by FAX equipment.

3) Cover Sheets

a. Users are responsible for ensuring each outgoing FAX transmission has a cover sheet clearly indicating the classification level, date and time of transmission, subject of the document, number of pages, and the sender's and addressee's name; organization; and FAX and office telephone numbers. **(See Supplementary Reference, Sample FAX Cover Sheet)**

b. The COMSEC Custodian must ensure that a log of all communications transmitted via a STU-III connection to a FAX machine is maintained in a central file for at least six months.

E552.5.4d Administrative Management of STU-III

1) Labeling

Labels and posters are available from the ISSO for USAID.

2) Logging Transmissions

At a minimum, the communications transmission log shall indicate the classification or sensitivity level, date, time, subject matter, and organizations and personnel sending and receiving FAX communications.

***552.6** Supplementary References

Approval to Access and Process Classified National Security Information via Automated Information System Equipment

Authorized Access List

Automated Information System Certification and Approval to Operate

Classified Processing Compliance Review

Contingency Planning for Information Resources

Sample Fax Cover Sheet

* **Selected Security Guidance**

USAID Classified Automated Information System User Agreement

Visitors Log

***552.7** Mandatory References

ADS 530

ADS 531

* **ADS 545**

ADS 550

ADS 561

ADS 562

ADS 565

ADS 566

ADS 567

ADS 568

* **Standard Form 312, Classified Information Nondisclosure Agreement**

12 FAM 090

12 FAM 500

12 FAM 540

* **12 FAM 630**

* **12 FAM 640**

Glossary Terms for 552

***classified national security information (classified information)**
Any data, file, paper, record, or computer screen containing information associated with the national defense or foreign relations of the United States and bearing the markings: confidential, secret, or top secret. (Chapters 545, 552)

***Compartmented**
The breaking down of sensitive data into small, isolated blocks to reduce the risk of unauthorized access. (Chapters 545, 552)

***Confidential**
A national security classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security (source: Executive Order 12958). (Chapters 545, 552)

***Dedicated Mode**
The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (Chapters 545, 552)

***encryption**
Protecting information by encoding it through use of logarithmic coding keys. (Chapters 545, 552)

***Secret**
A national security classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security (source: Executive Order 12958). An example of SECRET information is: Exact key length required by machine crypto system, excluding verification bits and redundancy (source: NTISSI 4002). (Chapters 545, 552)

***tempest**
The investigation, study, and control of compromising electromagnetic emanations from telecommunications and AIS equipment. Sometimes refers to system components that use approved emanation suppression/ containment systems for the processing and storage of classified national security information. (Chapters 545, 552, 562)

***Top Secret**
A national security classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave

damage to the national security (source Executive Order 12958). An example of TOP SECRET information is Information or evaluations which reveal vulnerabilities of a weapons system, communication security subsystems and associated storage media to attack (source:NTISSI 4002). (Chapters 545, 552)